

REMARKS

Claims 1, 3-5, 8-13, 15, 16, 19 and 20 remain pending. Claims 8, 15 and 19 are amended herein. No new matter has been added as a result of the amendments.

CLAIM REJECTIONS - 35 U.S.C. § 103(a)

The instant Office Action states that Claims 1, 3-5, 15-16 and 19-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Garcia et al (6,151,689) in view of Taguchi et al. (5,915,025). Applicants have reviewed the above-cited references and respectfully submit that the embodiments as recited in Claims 1, 3-5, 15-16 and 19-20 are patentable over Garcia in view of Taguchi for at least the following rationale.

Claim 1 recites (emphasis added):

creating a single data packet, including user data that is to be written in a write operation to said target storage device and key data that is used to establish authorization to store said user data, said key data being generated based upon a destination address of said write operation and based on a portion of said user data;

In the current Office Action, the Examiner agrees that Garcia fails to teach the claimed feature “said key data being generated based on a portion of the user data.”

Applicants submit that neither Garcia nor Taguchi, alone or in combination teach or suggest this claimed feature. Specifically, embodiments of the present invention enable simultaneous transmission of user data and key data in a single packet which decreases the time period for which the target device is vulnerable to an erroneous data transmission.

However, with Taguchi, the key data is not sent in a single data packet with the user data, as claimed. Taguchi provides details for how to generate key data. However, Taguchi actually teaches away from the claimed feature of a single data packet by teaching the key and the data are sent separately. In column 7, line 60 through column 8, line 6. Taguchi teaches "The encrypted data is placed in the storage means. When a request is made by the control means to process the encrypted data, the decryption key generation means generates the decryption key. This is very different from generating the key data based on the user data and sending it in a single data packet with the user data, as claimed.

For at least the foregoing rationale, Applicants respectfully submit that Claim 1, and similarly Claims 8 and 15 as amended, are patentable over Garcia in view of Taguchi under 35 U.S.C. § 103(a). As such, allowance of Claims 1, 3-5, 15-16 and 19-20 is respectfully requested.

Claims 8-13, 15-16, and 19-20 are rejected under 35 U.S.C. 103(a), as being unpatentable over Garcia et al (6,151,689) in view of Adler et al. (4,255,811). Applicants have reviewed the above-cited references and respectfully submit that the embodiments as recited in Claims 8-13, 15-16, and 19-20 are patentable over Garcia in view of Adler for at least the following rationale.

Applicants have amended Independent Claims 8 and 15 to include the feature “said key data being generated based upon a system clock setting of said computer system, based on a destination address of a write operation and based on a portion of said user data.” Applicants submit that neither Garcia nor Adler alone and in combination teach or suggest this claimed feature.

As stated above, Applicants submit that Garcia fails to teach or suggest the feature “said key data being generated based upon a destination address of said write operation and based on a portion of said user data.” Applicants further submit that Adler fails to remedy the deficiencies of Garcia.

Specifically, Adler fails to teach or suggest generating key data based on a destination address, as claimed. Adler is cited as teaching generating key data based on a system clock setting.

With the present claimed invention, key data is used to “establish authorization to store said user data.” Applicants would like to point out that the “key” of Adler is very different from the “key data” of the present claimed invention.

Adler may purport to teach an encryption key for encoding or decoding. However, Adler fails to teach or suggest key data to “establish authorization to store said user data,” as claimed. Because of this, Applicants submit that

modifying Garcia with Adler would significantly change the mode of operation of Garcia because the encryption scheme of Adler fails to correspond with Garcia's.

For at least the foregoing rationale, Applicants respectfully submit that Claim 8, and similarly Claim 15 as amended, are patentable over Garcia in view of Adler under 35 U.S.C. § 103(a). As such, allowance of Claims 8-13, 15-16, and 19-20 is respectfully requested.

CONCLUSION

In light of the above listed remarks, reconsideration of the rejected claims is requested. Based on the amendments and arguments presented above, it is respectfully submitted that Claims 1, 3-5, 8-13, 15, 16, 19 and 20 overcome the rejections of record, and that Claims 1, 3-5, 8-13, 15, 16, 19 and 20 are in a condition for allowance. Therefore, allowance of Claims 1, 3-5, 8-13, 15, 16, 19 and 20 is respectfully solicited.

Should the Examiner have a question regarding the instant amendment and response, the Applicants invite the Examiner to contact the Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,
WAGNER BLECHER LLP

Date: 08/22/2008

/John P. Wagner, Jr./

John P. Wagner, Jr.
Reg. No. 35,398
WESTRIDGE BUSINESS PARK
123 WESTRIDGE DRIVE
WATSONVILLE, CALIFORNIA 95076
(408) 377-0500